Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 7, 2015

R. Gagliano
K. Patel
B. Weis
Cisco Systems

March 6, 2015

BGPSEC Router Certificate Rollover
draft-ietf-sidr-bgpsec-rollover-03

Abstract

BGPSEC will need to address the impact from regular and emergency rollover processes for the BGPSEC End-Entity (EE) certificates that will be performed by Certificate Authorities (CAs) participating at the Resource Public Key Infrastructure (RPKI). Rollovers of BGPSEC EE certificates must be carefully managed in order to synchronize distribution of router public keys and the usage of those pubic keys by BGPSEC routers. This document provides general recommendations for that process, as well as describing reasons why the rollover of BGPSEC EE certificates might be necssary.

Status of this Memo

Copyright Notice

Table of Contents

1. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Introduction

In BGPSEC, a key rollover (or re-keying) is the process of changing a router's key pair (or pairs), issuing the corresponding new End-Entity certificate and (if the old certificate is still valid) revoking the old certificate. This process will need to happen at regular intervals, normally due to local policies at each network. This document provides general recommendations for that process. Certificate Practice Statements (CPS) documents MAY reference these recommendations. This process is comceptually similar to the RPKI Key Rollover process defined in [RFC6489].

When a router receives or creates a new key pair (depending on the key provisioning mechanism to be selected), this key pair will be used to sign new BGPsec_Path attributes [I-D.ietf-sidr-bgpsec-protocol] that are originated or that transit through the BGP speaker. Additionally, the BGP speaker MUST refresh its outbound BGPsec Update messages to include a signature using the new key (replacing the replaced key). When the rollover process finishes, the old BGPSEC certificate (and its key) will not longer be valid and thus any BGPsec Update that includes a BGPsec_Path attribute with a signature performed by the old key will be invalid. Consequently, if the router does not refresh its outbound BGPsec Update messages, routing information may be lost after the rollover process is finished. It is therefore extremely important that the BGPSEC router key rollover be performed such that the probability of new router EE certificates have been distributed throughout the RPKI before the router begin signing BGPsec_Path attributes with a new private key.

It is also important for an AS to minimize the BGPSEC router key rollover interval (i.e., in between the time an AS distributes an EE certificate with a new public key and the time a BGPSEC router begins to use its new private key). This can be due to a need for a BGPSEC router to distribute BGPsec_Path attributes signed with a new private key in order to invalidate BGPsec_Path attributes signed with the old private key. In particular, if the AS suspects that a stale BGPsec_Path attribute is being distributed instead of the most recently signed attribute it can cause the stale BGPsec_Path attribute to be invalidated by completing a key rollover procedure. The BGPSEC rollover interval can be minimized when an automated certificate provisioning process such as Enrollment over Secure Transport (EST) [RFC7030]) is used.

The Security Requirements for BGP Path Validation [RFC7353] also describes the need for protection against a replay attack, necessitating controlling BGPSEC's window of exposure to replay attacks. The BGPsec rollver method in this document can be used to

achieve this goal.

In [I-D.ietf-sidr-rtr-keying], the "operator-driven" method is introduced and it enables that a key pair could be shared among different BGP Speakers. In this scenario, the roll-over of the correspondent BGPSEC certificate will impact all the BGP Speakers sharing the same private key.

3. Key rollover in BGPSEC

A BGPSEC EE certificate (as any X.509 certificate) will required a rollover process due to causes such as:

BGPSEC scheduled rollover: BGPSEC certificates have an expiration date (NotValidAfter) that requires a frequent rollover process. The validity period for these certificates is typically expressed at the CA's CPS document.

BGPSEC certificate fields changes: Information contained in a BGPSEC certificate (such as the ASN or the Subject) may need to be changed.

BGPSEC emergency rollover Some special circumstances (such as a compromised key) may require the replacement of a BGPSEC certificate.

BGPSEC signature anti-replay protection An AS may determine stale BGPsec_Path attributes continue to be propogated

In most of these cases (probably excepting when the key has been compromised), it is possible to generate a new certificate without changing the key pair. This practice simplifies the rollover process as the correspondent BGP speakers do not even need to be aware of the changes to its correspondent certificate. However, not replacing the certificate key for a long period of time increases the risk that the certificate key may be compromised.

3.1. A proposed process for BGPSEC key rollover

The BGPSEC key rollover process will be dependent on the key provisioning mechanisms that would be in place. The key provisioning mechanisms for BGPSEC are not yet fully documented (see [I-D.ietf-sidr-rtr-keying] as a work in progress document). We will assume that an automatic provisioning mechanism suchas EST will be in place. The use of EST will allow BGPSEC code to include automatic re-keying scripts with minimum development cost.

If we work under the assumption that an automatic mechanism will exist to rollover a BGPSEC certificate, a possible process could be as follows.

1. New Certificate Pre-Publication: The first step in the rollover mechanism is to pre-publish the new public key in a new certificate. In order to accomplish this goal, the new key pair and certificate will need to be generated and published at the appropriate RPKI repository publication point. The details of

this process will vary as they depend on whether the keys are assigned per-BGP speaker or shared, whether the keys are generated on each BGP speaker or in a central location and wether the RPKI repository is locally or externally hosted.

2. Staging Period: A staging period will be required from the time a new certificate is published in the RPKI global repository until the time it is fetched by RPKI caches around the globe. The exact minimum staging time is not clear and will require experimental results from RPKI operations. RPKI repository design documents mention a lower limit of 24 hours (NOTE: need reference only one I found is the ops document). If rollovers will be done frequently and we want to avoid the stage period, an administrator can always provision two certificate for every router. In this case when the rollover operation is needed, the relying parties around the globe would already have the new keys. A staging period may not be possible to implement during emergency key rollover, in which case routing information may be lost.

3. Twilight: At this moment, the BGP speaker that hold the private key that has been rolled-over will stop using the OLD key for signing and start using the NEW key. Also, the router will generate appropriate BGPsec_Path attributes just as in the typical operation of refreshing out-bound BGP polices. This operation may generate a great number of BGPsec_Path attributes (due to the need to refresh BGP outbound policies). In any given BGP SPEAKER, the Twilight moment may be different for every peer in order to distribute the system load (probably in the order of minutes to avoid reaching any expiration time).

4. Certificate Revocation: This is an optional step. As part of the rollover process, a CA MAY decide to revoke the OLD certificate by publishing its serial number on the CA's CRL. On the other side, the CA will just let the OLD certificate to expire and not revoke it. This chose will depend on the reasons that motivated the rollover process.

5. RPKI-Router Protocol Withdrawals: Either due to the revocation of the OLD certificate or to the expiration of the OLD certificate's validation, the RPKI relying parties around the globe will need to communicate to their RTR peers that the OLD certificate's public key is not longer valid (rtr withdrawal message). It is not documented yet what will be a router's reaction to a RTR withdrawal message but it should include the removal of any RIB entry that includes a BGPSEC attribute signed with that key and the generation of the correspondent BGP WITHDRAWALs (either implicit or explicit).

The proposed rollover mechanism will depend on the existence of an automatic provisioning process for BGPSEC certificates. It will require a staging mechanism based on the RPKI propagation time of around 24hours, and it will generate BGPsec_Path attributes for all prefixes in the router been re-keyed.

The first two steps (New Certificate Pre-Publication and Staging Period) could happen ahead of time from the rest of the process as each network operators could prepare itself to accelerate a future key roll-over.

When a new BGPSEC certificate is generated without changing its key, steps 3 (Twilight) and 5 (RPKI-Router Protocol Withdrawals) SHOULD NOT be executed.

4. BGPSEC key rollover as a measure against replays attacks in BGPSEC

There are two typical generic measures to mitigate replay attacks in any protocol: the addition of a timestamp or the addition of a serial number. However neither BGP nor BGPSEC provide either measure. This section discusses the use of BGPSEC Rollover as a measure to mitigate replay attacks.

4.1. BGPSEC Replay attack window requirement

In [RFC7353] Section 4.3, the need to limit the vulnerability to replay attacks is described. One important comment is that during a windows of exposure, a replay attack is effective only if there was a downstream topology change that makes the signed AS path not longer current. In other words, if there have been no topology changes, then no security threat comes from a replay of a BGPsec_Path attribute (the signed information is still valid).

The BGPSEC Ops document [I-D.ietf-sidr-bgpsec-ops] gives some ideas of requirements for the size of the BGPSEC windows of exposure to replay attacks. At that document, it is stated that for the vast majority of the prefixes, the requirement will be in the order of days or weeks. For a very small but critical fraction of the prefixes, the requirement may be in the order of hours.

4.2. BGPSEC key rollover as a mechanism to protect against replay attacks

Since the window requirement is in the order of days (as documented in [I-D.ietf-sidr-bgpsec-ops]) and the BGP speaker re-keying is the edge router of the origin AS, it is feasible for a BGPSEC Rollover to mitigate mitigate. In this case it is important to complete the full process (i.e. the OLD and NEW certificate do not share the same key). By re-keying an AS is letting the BGPSEC certificate validation time be a sort of "timestamp" against replay attacks. However, the use of frequent key rollovers comes with an additional administrative cost and risks if the process fails. As documented before, re-keying should be supported by automatic tools and for the great majority of the Internet it will be done with good lead time to correct any risk.

For a transit AS that also originates BGPsec_Path attributes for its own prefixes, the key rollover process may generate a large number of UPDATE messages (even the complete Default Free Zone or DFZ). For this reason, it is recommended that routers in this scenario been provisioned with two certificates: one to sign BGPsec_Path attributes in transit and a second one to sign an BGPsec_Path attribute for prefixes originated in its AS. Only the second certificate (for prefixes originated in its AS) should be rolled-over frequently as a

means of limiting replay attach windows. The transit BGPSEC certificate is expected to be longer living than the origin BGPSEC certificate.

Advantage of Re-keying as replay attack protection mechanism:

1. All expiration policies are maintained in RPKI

2. Most of the additional administrative cost is paid by the provider that wants to protect its infrastructure (RP load will increase as there is a need to validate more BGPSEC certificates)

3. Can be implemented in coordination with planned topology changes by either origin ASes or transit ASes (e.g., if an AS changes providers, it completes a BGP Rollover)

Disadvantage of Re-keying as replay attack protection mechanism:

1. More administrative load due to frequent rollover, although how frequent is still not clear. Some initial ideas in [I-D.ietf-sidr-bgpsec-ops]

2. Minimum window size bounded by RPKI propagation time to RPKI caches for new certificate and CRL (2x propagation time). If pre-provisioning done ahead of time the minimum windows size is reduced (to 1x propagation time for the CRL). However, more experimentation is needed when RPKI and RPs are more massively deployed.

3. Increases dynamics and size of RPKI repository.

4. More load on RPKI caches, but they are meant to do this work.

5. IANA Considerations

No IANA considerations

6. Security Considerations

Several possible reasons can cause routers participating in BGPSEC to replace rollover their signing keys and/or signatures containing their current signature verification key. Some reasons are due to the usual key management operations reasons (e.g.,key exposure, change of certificate attributes, due to policy). However BGPSEC routers also may need to change their signing keys and associated certificate as an anti-replay protection.

The BGPSEC Rollover method allows for an expedient rollover process when router certificates are distributed through the RPKI, but without causing routing failures due to a receiving router not being able to validate a BGPsec_Path attribute created by a router that is the subject of the rollover.

7. Acknowledgements

We would like to acknowledge Randy Bush, Sriram Kotikalapudi, Stephen Kent and Sandy Murphy.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC6489] Huston, G., Michaelson, G., and S. Kent, "Certification Authority (CA) Key Rollover in the Resource Public Key Infrastructure (RPKI)", BCP 174, RFC 6489, February 2012.

8.2. Informative References

[I-D.ietf-sidr-bgpsec-ops] Bush, R., "BGPsec Operational Considerations", draft-ietf-sidr-bgpsec-ops-05 (work in progress), May 2012.

[I-D.ietf-sidr-bgpsec-protocol] Lepinski, M., "BGPsec Protocol Specification", draft-ietf-sidr-bgpsec-protocol-11 (work in progress), January 2015.

[I-D.ietf-sidr-rtr-keying] Patel, K. and R. Bush, "Router Keying for BGPsec", draft-ietf-sidr-rtr-keying-08 (work in progress), January 2015.

[RFC7030] Pritikin, M., Yee, P., and D. Harkins, "Enrollment over Secure Transport", RFC 7030, October 2013.

[RFC7353] Bellovin, S., Bush, R., and D. Ward, "Security Requirements for BGP Path Validation", RFC 7353, August 2014.

Authors' Addresses

Roque Gagliano
Cisco Systems
Avenue des Uttins 5
Rolle, VD 1180
Switzerland

Email: rogaglia@cisco.com

Keyur Patel
Cisco Systems
170 W. Tasman Driv
San Jose, CA 95134
CA

Email: keyupate@cisco.com

Brian Weis
Cisco Systems
170 W. Tasman Driv
San Jose, CA 95134
CA

Email: bew@cisco.com